Perspective patronale en droit de l'emploi et relations de travail
Labour and Employment Law for Employers

Emond Harnden LLP

Employee Privacy Exposed

Steven Williams

Raquel Chisholm

February 15, 2006

www.emondharnden.com

Overview

1. Legislation
2. The Duty to Accommodate
3. Electronic Monitoring
4. Proper Video Surveillance
5. Security Clearance Screening

PIPEDA

- PIPEDA applies to:
  - Employee information of a federal work, undertaking, or business
- PIPEDA does not apply to:
  - The employee information of provincially regulated private organizations

PIPEDA

- PIPEDA defines “personal information” in a very broad fashion:
  - *"personal information" means information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization.*

Ontario's Freedom of Information and Protection of Privacy Acts

- Freedom of Information and Protection of Privacy Act (FIPPA) and Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) apply to provincial public bodies
- Examples:
  - FIPPA – Colleges, Ministry of Labour
  - MFIPPA – Municipalities, School Boards
- Protects the privacy of individuals with respect to personal information about themselves held by these public institutions, including a right of access

Ontario's Freedom of Information and Protection of Privacy Acts

- The Ontario Information and Privacy Commissioner has made several rulings as to whether employee information is "personal information"
- Employee information may not constitute personal information if it:
  - Relates to the employment responsibilities, position, activities
  - Identifies an individual in his or her employment, professional or official capacity, or provides a business address or telephone number
  - Constitutes opinions developed or expressed by an individual in his or her employment, professional or official capacity, or information about other normal activities undertaken in that context

Ontario's Freedom of Information and Protection of Privacy Acts

- Employee information may constitute personal information when it:
  - Involves an evaluation of the employee's performance or an investigation into his or her conduct
  - Concerns activities that extend beyond the routine, day-to-day responsibilities of their employment (eg. Attendance at a training course)
  - Is information pertaining to a complaint against the conduct of an individual in practising his or her profession or occupation
  - Alleges misconduct in their employment capacity or where conduct has been called into question.

Privacy Act (Federal)

- Applies to personal information held by federal government institutions that are not covered by PIPEDA
- Defines “personal information” as information about an identifiable individual that is recorded in any form and provides an extensive non-exhaustive list which includes:
  - Information relating to the education or the medical, criminal or employment history of the individual
  - The views or opinions of another individual about the individual

Privacy Act (Federal)

- The Treasury Board has also adopted an “Employee Privacy Code” concerning the collection, use, and disclosure of personal information that takes into account the principles and spirit of the Privacy Act and general privacy principles.

Ontario's Personal Health Information Protection Act ("PHIPA")

- Primarily applies to the handling of personal health information by "health information custodians" and their "agents"
- Directed specifically at the protection of an individual's medical information.
- Establishes a set of uniform rules about the collection, use, and disclosure of personal health information

Ontario's Personal Health Information Protection Act ("PHIPA")

- May apply to Ontario employers as per the "recipient rule" (s.49)
- If an employer receives medical information from a health information custodian, the legislation stipulates it may only be used or disclosed for the purpose to which the employee originally consented
- PHIPA does not apply to information employers receive directly from employees

When No Legislation Applies…

- For many Ontario employers, privacy legislation does not apply to their employment relationships.
- Does this matter? Human rights law and other labour and employment laws have embedded privacy principles into them. Arbitrators and adjudicators have also utilized these principles in their awards.

When no legislation applies …
Somwar v. McDonald's Restaurants

- A January 10th 2006 decision of the Ontario Superior court has noted that a civil remedy for invasion of privacy *may* exist.
- The court in this case did not allow a motion to dismiss an employee's claim against their employer for invading his right to privacy
- In reviewing the available jurisprudence, the court concluded that *"it is **not** settled law in Ontario that there is no tort of invasion of privacy….the time has come to recognize invasion of privacy as a tort in its own right."*

When no legislation applies …

- Therefore, notwithstanding issues over jurisdiction of certain privacy statutes and their applicability to employee information, employers should always remain cognizant of all the privacy principles

Privacy Law & The Duty to Accommodate

- Employers are obligated to make workplace adjustments (duties, tasks, demands, hours, methods) in order to accommodate an employee with a disability

- Personal health information is essential for a mutually satisfactory and successful accommodation process:
  - To ensure a safe return to work
  - To confirm the extent of an employee's limitations, restrictions, and capabilities, and make workplace changes accordingly
  - To adequately address the employee's needs

Privacy Law and the Duty to Accommodate: Legislation

- As noted, PIPEDA defines “personal information” broadly, but includes a specific definition for “personal health information”
- FIPPA and MFIPPA define personal information to include “information relating to .. the medical, psychiatric .. history.”
- The definition in PHIPA, “relates to the physical or mental health of the individual” would likely encompass most information related to the accommodation effort.
- The Privacy Act contains a similar inclusion into its definition of “personal information”: information “relating” to “medical.. history”

Limits on Requested information

- Generally speaking, a *prognosis* or information regarding job-related limitations and capabilities would satisfy the purpose of facilitating an accommodation or ensuring a safe return to work
- A *diagnosis* or complete medial history would likely be excessive under privacy principles as it may not be relevant to or necessary for planning an accommodation or ensuring a safe return to work
- Any health information unrelated to this purpose or the performance of the employee's duties would be an excessive information request

Accommodation: It's a two-way street

- Without your employee's **consent**, you will not be able to obtain the medical information you require for the accommodation process.
- An employee may be entitled to withhold consent if the employee feels the information being requested exceeds the "purposes" or achieving accommodation or safe return to work
- But the employee is an integral player in the accommodation process, and the unwarranted failure to facilitate or cooperate in the process may frustrate the accommodation effort and lead to an unsuccessful human rights complaint or grievance

Information on a "Need to Know" Basis

- Even though certain statutes (eg. FIPPA/MFIPPA) stipulate that a record should be in permanent format to be "personal information" for the purposes of disclosure protections, your organization should be mindful of conversations as well as formal documentation
- Employers should endeavour to determine the *minimum* degree of disclosure necessary to achieve a successful employee accommodation
- An employee's medical information should be provided only to those who absolutely need to be aware of the information

PIPEDA Case Summary # 257

FACTS

- Two complainants worked in high-risk, safety-sensitive positions.
- To support a sick leave absence, the company requested a medical certificate, which was to include a medical diagnosis.
- The employees, while acknowledging the employer had the right to inquire into what restrictions might prevent them from doing their jobs safely and verify their fitness for such work, felt the request for a diagnosis was unreasonable.
- In the circumstances of the case, the Commissioner concluded the complaint was **well founded**

Greater Toronto Airport Authority & PSAC (Fed Arb-2004)

FACTS

- The grievor sought to return to work after a quadruple heart surgery
- The employer required medical information concerning the grievor's health condition to understand the extent of his limitations and capabilities
- The accommodation process was unduly prolonged due to difficulties the employer encountered in securing the personal health information it required
- The grievor actively restricted the scope and extent of the medical information being released, and interfered with communications between the employer and his physician

Greater Toronto Airport Authority & PSAC (Fed Arb-2004)

- The arbitrator stated as follows:

  "One may admire the grievor for his strong feelings about divulging medical information but there is a price that goes along with it….in order to satisfy [the employer's] obligation, the employer must not be prevented from communicating with the employee's physician so as to prevent it from sufficiently satisfying its concerns about the employee's capabilities of performing work assigned to him."

Electronic Monitoring

- Employers can review the use of their technology to ensure a positive and productive working environment.
- Internet misuse can result in system overload, lost productivity, network security risks, employer liability, and the presence of obscene and offensive content in the work environment.
- However, employees usually consider their e-mail messages and computer use to be private.

Electronic Monitoring: Purposes, Consent & Limiting Collection

- An employer must have a “reasonable” legitimate purpose for collecting the information:
  - Protection of both the employer and employees against the threat of harassment and liability associated with misuse of network facilities
  - Prevention of dissemination of discriminatory or other offensive material and network security
- Ensure employees are aware of these purposes through an established IT Use policy

Electronic Monitoring: Purposes, Consent & Limiting Collection

- Policies should:
  - State a reasonable purpose and scope for prospective monitoring and/or data collection.
  - Employer reserves the right (but assumes no duty) to view, log, record, monitor and/or block all online activity, including email and internet, at all times during the employment relationship (no reasonable expectation of privacy)
  - Set limits on what constitutes appropriate and inappropriate system use,
  - Contain a **written consent** executed by each employee.
  - Specify the consequences of breaches of the policy

Electronic Monitoring: Purposes & Limiting Collection

- Limit collection to what is necessary to achieve the prescribed purposes. Continuous surveillance is not advisable.
- Remind employees that they are being monitored (eg. at login).
- Review your collective agreement for any monitoring restrictions.

E-mail: Is it inherently private?

- *Camosun College* (1999 – British Columbia): is email private?

  The potential for dissemination is limited only by the internet....The nature of the medium therefore does not support a claim for confidentiality. Rather, it prevents any such a claim."

- Arbitrator said any reasonably informed email user would know that messages could be monitored and the originator has no control over the circulation of the message.

Privacy Act Findings (April 2004): Inappropriate monitoring of employees' e-mail

FACTS

- Two employees questioned management's authority to retrieve copies of e-mail messages they had written each other regarding a *Privacy Act* complaint.
- One of the employees had discovered performance evaluations about several co-workers on the local computer network and notified her union's representative.
- Management fixed this problem, but also initiated an inquiry to establish whether any disciplinary action should be taken against the employee for disclosing this information to the union representative.

Privacy Act Findings (April 2004): Inappropriate monitoring of employees' e-mail

FACTS

- Decided to retrieve the e-mail messages for this purpose, *not* for any concern that the employees were improperly using the system
- The employer did not have a formal policy on the use of electronic networks

Privacy Act Findings (April 2004): Inappropriate monitoring of employees' e-mail

FINDINGS

- Unnecessary to retrieve the e-mail exchanges to determine if disciplinary action was warranted
- The employer's actions could not be justified under the Privacy Act
- Recommended the employer proceed quickly to complete its internal disciplinary inquiry and that it publish a policy governing the use of its electronic networks.

Owens Corning Canada Ltd. & UNITE-HERE (2005 Ontario Arb)

FACTS

- Grievor discharged for personal computer use contrary to the company's computer use policy
- The inappropriate use included the materials he accessed or attempted to access and the time he spent accessing or attempting to access websites on the internet while at work.
- To monitor internet use the company purchased a commercial software package that blocked access to pornographic sites, and records activity in a manner described as "taking snapshots of use."

Owens Corning Canada Ltd. & UNITE-HERE (2005 Ontario Arb)

FACTS

- As part of this program, the company set a daily threshold for attempted access to blocked sites. When this threshold is exceeded, a report was generated detailing the individual's computer use.

DECISION

- An employer has the right to discipline an employee for using its computer system to access via internet or e-mail inappropriate content
- The software takes snapshots of use, and does not record actual computer activity in between those snapshots.
- His personal internet use was contrary to the policy and he engaged in these activities during working hours

Proper Video Surveillance

- Legitimate business interests or collection "purpose" must be identified: eg. theft deterrence, safety of employees, security of employer property.
- It must also be proven that video surveillance will achieve or address this purpose/concern.
- To effectively balance operational requirements with employee privacy interests, employers must ensure less-intrusive measures have been canvassed

Proper Video Surveillance

- Employees need to be informed that the employer will be engaging in video surveillance and the purposes for doing so.
- Surreptitious surveillance will often constitute privacy infringement
- Collection of information must be limited to what is reasonable to achieve this purpose. The way the cameras are deployed must be considered:
  - Continuous surveillance and retention of all recorded images is not advisable
  - Ensure monitoring is not conducted in areas unnecessary to the noted purpose

Information and Privacy Commissioner (Ontario) Guidelines

- Should only be considered after other measures of deterrence of detection have been considered and rejected as unworkable (substantially less effective or not feasible).
- The benefits of surveillance need to substantially outweigh the reduction of privacy.
- The use of *each* video surveillance camera should be justified on the basis of verifiable specific reports, incidents of crime, or significant safety concerns.

Information and Privacy Commissioner (Ontario) Guidelines

- The proposed design and operation minimizes privacy intrusion to that which is absolutely necessary to achieve its goals.
- Set out an appropriate retention period for recorded information.
- Limit access to storage devices of the recorded information to authorized personnel (a log should be kept) and kept confidential.

Information and Privacy Commissioner (Ontario) Guidelines

- Surveillance conducted by means of hidden devices should only be used as an absolute last resort
- Ensure only pertinent information is collected and that cameras are not used for any other purpose than was originally intended.
- Proper notice that an area is subject to surveillance is necessary

Eastmond v. CP Railway (Federal Court; 2004)

FACTS

- The Canadian Pacific Railway ("CP") installed 6 digital recording surveillance cameras in their mechanical facility area at Scarborough, Ontario to:
  - reduce vandalism/theft,
  - reduce CP's potential liability for property damage
  - provide security for staff
- Eastmond, an employee of CP and a member of CAW-Local 1001, made a complaint to the Privacy Commissioner of Canada

Eastmond v. CP Railway (Federal Court; 2004)

- In examining Eastmond's complaint, the Privacy Commissioner set out a four part test to determine whether CP's use of the video cameras was reasonable:
  1. Is the measure demonstrably necessary to meet a specific need?
  2. Is it likely to be effective in meeting that need?
  3. Is the loss of privacy proportional to the benefit gained?
  4. Is there a less privacy-invasive way of achieving the same end?

Eastmond v. CP Railway (Federal Court; 2004)

- The Privacy Commissioner held that Eastmond's complaint was well founded. A reasonable person ***would not*** consider the circumstances sufficient to warrant this intrusive measure;
  1. A demonstrable need for the cameras had not been proven;
  2. Adverse psychological effects due to the privacy invasion could be occurring;
  3. Other alternatives existed (eg. Increased lighting) to meet CP's purposes for the video cameras;

Eastmond v. CP Railway (Federal Court; 2004)

- The Federal Court of Canada adopted the same four-part test but determined that a reasonable person ***would*** consider CP's purposes appropriate in the circumstances:
  1. The court held that "*CP has established a legitimate need to have the cameras installed where they were ….*"
  2. The court held that the camera surveillance and recording *would* likely be effective in meeting its need.

Eastmond v. CP Railway (Federal Court; 2004)

3. On the third part of the test, the court held that *"the loss of privacy is proportional to the benefit gained,"* and highlighted the following points:
   - the collection of personal information is not surreptitious. Warning signs are displayed.
   - The collection of personal information is not continuous and is not limited to CP employees. The collection is not intended to measure work performance
   - the recorded images are locked up and only accessed by responsible managers and CP police, and *only* if there is an incident report. If there are no incidents recorded, the recordings are destroyed within an appropriate time frame.

Eastmond v. CP Railway (Federal Court; 2004)

4. The court held that it was satisfied that CP had looked at all alternatives and concluded that these measures were not cost effective and would be disruptive to CP's operations

Video Surveillance & Labour Relations

- The federal court in *Eastmond* noted that these factors are those which arbitrators have taken into account in balancing privacy interests of employees with the legitimate interests of employers. (eg. *Unisource Canada – 2003 121 LAC (4th) 437)*
- *"[arbitrators] have taken a reasonableness approach to the admissibility of surreptitiously gathered videotape evidence. In such instances, arbitrators assess first whether the surveillance of an employee's activity was reasonable, and second, whether the surveillance was conducted in a reasonable manner, proportional to the employer's legitimate interests."* - Canadian Labour Arbitration (Brown and Beatty)

Security Checks: Limiting Collection, Consent, & Purposes

- The nature of the employer's business will be considered in determining what information collection and purpose is "reasonable"
- For example, the more security sensitive the business is, the greater the permissible degree of privacy infringement: this speaks to the "balance" between employee privacy and operational requirements
- While consent is still required, refusing a "reasonable" information request may be a legitimate basis for employer action
- A choice between giving consent to the security check and losing your job or being transferred is not a great choice, but still a choice.

PIPEDA Case Summary # 232

FACTS

- The employer, a nuclear facility, was licensed by the Canadian Nuclear Safety Commission (CNSC)
- Following terrorist attacks in the US, the CNSC required all employees to have a facility-access security clearance.
- Spousal/Partner information was to be used in the security screening process without consent of the spouse/partner

DECISION

- A reasonable person would find it appropriate for the CNSC to order its licensees to not permit any person without proper clearance to enter their facility.

PIPEDA Case Summary # 232

DECISION

- Given that a security check involves a review of as many aspects of the employee's life as possible, it would be inappropriate not to conduct an investigation into the spouse's background
- The purpose of the check is to identify potential threats to nuclear installations – spousal or partner information is key to achieving that goal and collection of this information is appropriate.
- It is not appropriate to obtain separate consent from the spouse / partner – the onus is on the employee to seek this consent. Should they not provide consent, the employee would need to review options, such as seeking alternative employment.

Questions?